REMARKS

In response to the non-final Office action of July 21, 2005, applicant asks that all claims be allowed in view of the above amendment to the claims and the following remarks.

Claims 1-92 are now pending, of which claims 1, 19, 32, 50, 63 and 79 are independent. Claims 1, 19, 32, 50, 58, 63, 78 and 79 have been amended. Support for these amendments may be found, for example, in original claims 8-12. Claim 78 has been amended to depend from claim 75. No new matter has been introduced.

Rejections under 35 U.S.C. §102(b)

Claims 1-92 have been rejected under 35 U.S.C. §102(b) as being anticipated by Cane (U.S. Patent No. 5,416,840). Applicant requests reconsideration and withdrawal of the rejection of claims 1-92 because Cane does not describe or suggest the subject matter of the independent claims. For example, Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claims 1, 19, 32, 50, 63 and 79. Nor does Cane describe or suggest designating a client communication system as unauthorized based on a result of the claimed mathematical computation, as recited in independent claims 1, 32 and 63.

Claims 1-18, 32-49 and 63-78

Independent claim 1, as amended, recites a method for determining whether a client communication system seeking access to a host communication system is authorized to do so. The method includes performing a mathematical computation[1] on an access password and a client-communication-system-specified identifier. The client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system. The method also includes designating a client communication system as unauthorized based on a result of the mathematical computation.

---

1 The Office Action asserts that a mathematical computation, as recited in claim 1, is the same as an algorithm. See Office Action of July 21, 2005 at page 2 (stating "...to perform a mathematical computation (i.e. algorithm")). Applicant respectfully disagrees that a mathematical computation is necessarily an algorithm.

In contrast, Cane describes techniques for "locking" personal computer software that is distributed on CD-ROM or over a network, where the "locking" prevents total or partial access to the software by a user who has not purchased the software, and later "unlocking" the software once the user purchases the software. See Cane at col. 3, lines 21-38. To enable such locking, Cane discloses encrypting software and storing, in a table (called a "software-encryption key table" or a "software-key table"), a software identifier associated with the software encryption key used to encrypt the software. See Cane at col. 5, lines 28-30 and col. 6, lines 17-29. The software-key table is used to identify the software encryption key that had been used to encrypt the particular software that is to be unlocked for installation and use by a purchaser. See Cane at col. 6, lines 24-29 and col. 3, lines 28-35.

Cane also discloses a personal computer decryption device (referred to as a "PCDD") that is included in a computer on which the software is to be installed and used. See Cane at col. 4, line 8-14 and FIG. 1. The personal computer decryption device stores a hardware identifier and a password key. See Cane at col. 4, lines 15-22, and FIG. 2. The personal computer decryption device is used to decrypt the software so that the software can be installed and used on the computer in which the personal computer decryption device resides. See Cane at col. 3, lines 35-38, and col. 4, lines 1-2, 26-37.

Notably, Cane indicates that, in a preferred embodiment, the password key bears "no algorithmic relationship to the hardware identifier." See Cane at col. 4, lines 22-25 (emphasis added). Cane uses a table (called a "hardware-password key table" or a "serial number-key table") to store the association of a hardware identifier and the password key that both are stored on a personal computer decryption device. See Cane at col. 5, lines 25-30, and col. 6, lines 18-32. Cane's serial number-key table is later used to determined a password key that corresponds to a particular hardware identifier. See Cane at col. 3, lines 22-25; col. 5, lines 25-30; and col. 6, lines 18-32.

In general, Cane's process for unlocking software includes generating an encrypted password that is sent to the user's computer and using the personal computer decryption device of the user's computer to decrypt the password, which is then used to decrypt and "unlock" the software. See Cane at col. 3, lines 28-38 and col. 4, lines 27-36. See also Cane at FIG. 4 (illustrating a flow diagram of a preferred environment in which a software vendor 400 provides

encrypted software to a publishing center 401, which, in turn, provides encryption key and software identifier information to an order center 402, which provides a user 404 with a password to unlock the software after purchase) and col. 5, lines 19-43 (describing the flow between the entities of FIG. 4).

More particularly, Cane's process for unlocking software includes generating a password using a software encryption key and a password key. See Cane at col. 6, lines 31-38 and col. 7, lines 64-67. See also Cane at col. 4, lines 27-36. The particular software encryption key to be used corresponds to the software to be unlocked and is determined by looking up, in the software-key table, the software identifier of the software to be unlocked. See Cane at col. 6, lines 31-34 and col. 4, lines 27-34. The particular password key to be used corresponds to the password key stored on the personal computer decryption device of the computer on which the software to be unlocked resides, and the particular password key is determined by looking up, in the serial number-key table, the hardware identifier stored in the personal computer decryption device. See Cane at col. 6, lines 31-34 and col. 4, lines 27-34. Presumably, the software encryption key is encrypted with the password key. In any event, the encrypted password is sent to the user's computer, and the personal computer decryption device decrypts, using its stored password key, the password, which "recovers" the software encryption key. See Cane at col. 5, lines 5-7 and col. 6, lines 45-53. The software encryption key then is used to decrypt the software. See Cane at col. 6, lines 54-58.

As such, Cane discloses a password that is generated based on a software encryption key and a password key, neither of which being specific to the client communication system used to store data to be unlocked by these keys. Moreover, the software encryption key is a cryptographic key that used to encrypt and decrypt the software, and, hence, the software encryption key is not a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in amended claim 1. The password key is a cryptographic key that is used to encrypt and decrypt the generated password, and, hence, the password key is not a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Accordingly, Cane's generation of the password does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system. Nor does Cane's decryption process, which operates on the generated password using the password key stored in the personal computer decryption device, describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Moreover, while Cane discloses that the hardware identifier of a particular personal computer decryption device is looked-up using the serial number-key table identifier to determine the password key stored on the personal computer decryption device, Cane does not describe or suggest encrypting, decrypting or otherwise performing a computation on a hardware identifier stored in a personal computer decryption device.

In another aspect, Cane discloses decrypting, using the password key, an authorization code associated with the software and using the decrypted authorization code to trigger the generation of a message digest that is used to authorize the running of previously decrypted software. See Cane at col. 6, line 59 to col. 7, line 37. This aspect of Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, as recited in claim 1. Nor does the Office action contend that this portion of Cane does so.

Accordingly, Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in amended claim 1. Because Cane does not perform the claimed mathematical computation, Cane necessarily cannot describe or suggest designating a client communication system as unauthorized based on a result of the claimed mathematical computation, also as recited in claim 1.

For at least these reasons, applicant respectfully requests withdrawal of the rejection of independent claim 1, along with claims 2-18 that depend therefrom.

Independent claim 32 recites a computer readable medium or propagated signal having embodied thereon a computer program for identifying an unauthorized client communication system seeking access to a host communication system in a manner corresponding to that of independent claim 1, and independent claim 63 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 32 and 63, along with claims 33-49 and claims 64-78 that depend therefrom.

Claims 19-31, 50-62 and 79-92

Independent claim 19 recites a method for handling information about an authorized client communication system. The method includes, *inter alia*, performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 19, along with claims 20-31 that depend therefrom.

Independent claim 50 recites a computer readable medium or propagated signal having embodied thereon a computer program for handling information about an authorized client communication system in a manner corresponding to that of independent claim 19, and independent claim 79 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 50 and 79, along with claims 51-62 and 81-92 that depend therefrom.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be

exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant submits that all claims are in condition for allowance.

Pursuant to 37 CFR §1.136, applicant hereby petitions that the period for response to the action dated July 21, 2005, be extended for one month to and including November 21, 2005.

Please apply the amount of $120.00 for the Petition for Extension of Time fee to Deposit Account Number 06-1050.

Please apply any other charges or credits to Deposit Account Number 06-1050.

Respectfully submitted,

Date: November 21, 2005

Barbara A Benoit

Barbara A. Benoit
Reg. No. 54,777

Customer No.: 26171
Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331